(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2002 (10.01.2002)

PCT

(10) International Publication Number
WO 02/03196 A2

(51) International Patent Classification⁷: G06F 9/00

(21) International Application Number: PCT/US01/19325

(22) International Filing Date: 14 June 2001 (14.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/608,551 30 June 2000 (30.06.2000) US

(71) Applicant *(for all designated States except US)*: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: GRAWROCK, David [US/US]; 8285 Southwest 184th Avenue, Aloha, OR 97007 (US).

(74) Agent: MALLIE, Michael, J.; Blakely, Sokoloff, Taylor & Zafman, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

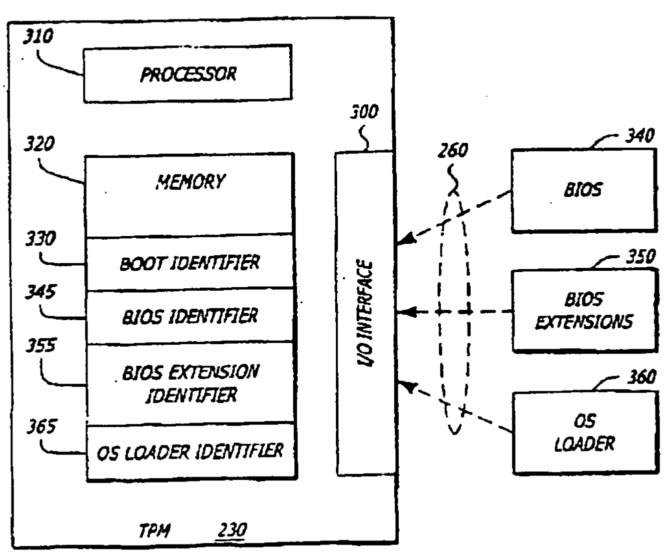
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PROTECTION OF BOOT BLOCK DATA AND ACCURATE REPORTING OF BOOT BLOCK CONTENTS



(57) Abstract: In one embodiment, an integrated circuit device comprises a trusted platform module and a boot block memory unit covered by a common package. The boot block memory unit is in communication with the trusted platform module and provides boot information to the trusted platform module. An example of the boot information includes a boot block code.

WO 02/03196 A2

PROTECTION OF BOOT BLOCK DATA AND ACCURATE REPORTING OF BOOT BLOCK CONTENTS

1. Field

This invention relates to the field of data security. In particular, the invention relates to an apparatus and method for protecting information and accurately reporting this information within an electronic system.

2. Background

Personal computers (PCs) typically include different types of storage components to store programs and data. These storage components include random access memory (RAM), read-only memory (ROM), and memory devices that are located external to the PC (e.g., hard disk or a floppy disk). To load an operating system on a PC, it is necessary to initialize or "boot" the PC by loading and executing boot code. Because the PC typically is unable to access external devices until after it is booted, the boot code is stored internally within the PC.

Typically, a ROM component is used to store the boot code. This boot code, normally referred to as "boot block," is obtained from the ROM and executed. The boot block is coded to (i) locate Basic Input/Output System (BIOS), (ii) load the BIOS for execution, and (iii) pass control to the BIOS. In addition, current platform developments may now require the boot block to report each step of the boot process to a hardware device referred to as a "trusted platform module" (TPM). Defined by the Trusted Computing Platform Alliance, the TPM records the operations of the boot process for subsequent verification by a challenger that the boot process occurred as expected. This poses a number of disadvantages.

For example, the boot block would now need to reliably report the steps of the boot process to the TPM. Thus, to ensure reliable transfer of this data, the boot block would likely require data processing functionality in order to perform cryptographic operations on the data before submission to the TPM.

Additionally, this communication protocol between the boot block and the TPM would be trustworthy only if the boot block is unchangeable. However, this protocol is unable to detect modifications to information regarding the boot process originating from the boot block or replacement of the ROM itself.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is an exemplary embodiment of a platform practicing the invention.

Figure 2 is an exemplary embodiment of the packaged IC device employed within the platform of Figure 1.

Figure 3 is an exemplary embodiment of the TPM of Figure 2.

Figure 4 is an exemplary embodiment of a flowchart illustrating the operations during initialization of the platform of Figure 1.

DESCRIPTION

The present invention relates to an apparatus and method for protecting information and accurately reporting this information within an electronic system. More specifically, the invention comprises the act of binding the TPM to a boot block memory device. This binding, which may be physical or logically through cryptographic mechanisms, allows the TPM to accurately report the identity of the boot block without reliance on any intervening devices.

Herein, certain details are set forth in order to provide a thorough understanding of the present invention. It is apparent to a person of ordinary skill in the art, however, that the present invention may be practiced through many embodiments other that those illustrated. Well-known circuits are not set forth in detail in order to avoid unnecessarily obscuring the present invention.

In the following description, certain terminology is used to discuss features of the present invention. For example, a "platform" includes any product that performs operations for subsequent analysis and verification of the platform's boot process. Examples of the platform include, but are not limited or restricted to a computer (e.g., desktop, a laptop, a server, a workstation, a personal digital assistant or other hand-held, etc.); communication equipment (e.g., wireless handset, facsimile, etc.); a television set-top box and the like. A "link" is broadly defined as one or more information-carrying mediums such as electrical wire, optical fiber, cable, trace, or even a wireless channel using infrared, radio frequency (RF), or any other wireless signaling mechanism.

In addition, the term "information" is defined as one or more bits of data, address, and/or control. A "software module" includes code that, when executed, performs a certain function. Examples of a software module include an application, an applet, or even a series of code instructions, possibly a subset of code from an applet, acting as a lesser sized software module.

A "cryptographic operation" is an operation performed for additional data security. For example, one type of cryptographic operation involves digital signing information to produce a digital signature. This digital signing operation may be in accordance with Digital Signature Algorithm (DSA). Another type of cryptographic operation involves hashing, namely a one-way conversion of information to a fixed-length representation. Often, this representation, referred to as a "hash value" or an "identifier", is substantially less in size than the original information. It is contemplated that, in some cases, a 1:1 conversion of the original information may be performed.

Referring to Figure 1, an exemplary block diagram of an illustrative embodiment of a platform 100 employing the present invention is shown. The platform 100 comprises a processor 110, a memory control hub (MCH) 120, a system memory 130, an input/output control hub (ICH) 140, and a packaged integrated circuit (IC) device 150 which initiates and monitors the boot process of the platform 100. The packaged IC device 150 features a boot block memory unit 220 and a trusted platform module 230 as described in Figure 2.

As shown in Figure 1, the processor 110 represents a central processing unit of any type of architecture, such as complex instruction set computers (CISC), reduced instruction set computers (RISC), very long instruction word (VLIW), or a hybrid architecture. In one embodiment, the processor 110 is compatible with the Intel® Architecture (IA) processor, such as the IA-32 and the IA-64. Of course, in an alternative embodiment, the processor 110 may include multiple processing units coupled together over a common host bus 105.

Coupled to the processor 110 via the host bus 105, the MCH 120 may be integrated into a chipset that provides control and configuration of memory and input/output devices such as the system memory 130 and the ICH 140. The system memory 130 stores system code and data. The system memory 130 is typically implemented with dynamic random access memory (DRAM) or static random access memory (SRAM).

The ICH 140 may also be integrated into a chipset together or separate from the MCH 120 to perform I/O functions. As shown, the ICH 140 supports communications with the packaged IC device 150 via link 160. Also, the ICH 140 supports communications with components coupled to other links such as a Peripheral Component Interconnect (PCI) bus at any selected frequency (e.g., 66 megahertz "MHz", 100 MHz, etc.), an Industry Standard Architecture (ISA) bus, a Universal Serial Bus (USB) or another bus configured with a different architecture than those briefly mentioned.

Of course, it is contemplated that the packaged IC device 150 may be employed in a different embodiment than described above. For example, the packaged IC device 150 may be employed within the ICH 140. Thus, the package associated with this embodiment is the package that protects other integrated circuit(s) associated with the functionality of the ICH 140.

Referring to Figure 2, an exemplary embodiment of the packaged IC device 150 is shown. The packaged IC device 150 comprises one or more integrated circuits placed within a protective package 200 such as an IC package, a cartridge covering a removable daughter card and the like. For this embodiment, the packaged IC device 150 comprises a single integrated circuit 210 featuring a boot block memory unit 220 in communication with a trusted platform module (TPM) 230 over a link 240. This single integrated circuit implementation increases the difficulty in monitoring communications between the boot block memory unit 220 and the TPM 230. Of course, although not shown, it is contemplated that the boot block memory unit 220 and the TPM 230 may be implemented as separate integrated circuits.

As shown, the boot block memory unit 220 provides both boot services 250 during initialization and boot information to the TPM 230. For example, the "boot services" may include a root of trust such as a boot block code executed at the start of the initialization process of the platform 100 to locate, load and pass control to the BIOS for example. However, it is contemplated, however, that the entire BIOS may be substituted for the boot block code described above. The "boot information" may be an image of the boot block code or multiple sub-images that collectively represent the boot block code, which is used to monitor the boot process.

Referring now to Figure 3, an exemplary embodiment of the TPM 230 of Figure 2 is shown. The TPM 230 comprises an input/output (I/O) interface 300, a processor 310, and memory 320 (e.g., volatile and/or non-volatile). Herein, the processor 310 is

configured to access certain content within the memory 320 (e.g., software modules, keying material, etc.) to perform cryptographic operations on incoming information. For example, as the TPM extracts the boot information from the boot block memory unit 220 (or even subsequent to that extraction), the processor 310 performs a hash operation on the boot information to produce a boot identifier 330. The boot block identifier 330 is stored in memory 320. For one embodiment, the boot block identifier 330 is calculated for each start-up of the platform 100. In another embodiment, however, the boot block identifier 330 is calculated for a first start-up and retained in non-volatile memory for subsequent use for later start-ups. This is a less secure, but less intensive from a processing standpoint.

Similarly, during initialization, various software modules are provided to the TPM 230. Examples of the modules include BIOS 340, Option ROMs such as BIOS extensions 350, or even a OS loader 360 which is a portion of the operating system that is loaded into the system memory 130 to control loading of the operating system. As an option, these modules 340, 350 and 360 can undergo a hash operation to produce corresponding identifiers 345, 355 and 365 for later use in verification by a challenger.

The TPM 230 further responds to inquiry requests from a challenger. A "challenger" may be any electronic device within the platform or even external to the platform. The "inquiry request" may be in the form of a challenge message, namely information encrypted with keying material (e.g., a public key of TPM, symmetric key, etc.) accessible by the TPM 230. In response, the TPM 230 provides TPM services such as a digital signature featuring the boot block identifier 330, keying material, certificates and the like.

Referring to Figure 4, a flowchart illustrating the operations during initialization of the platform 100 of Figure 1 is shown. Initially, the packaged IC device is directly attached to a substrate of a platform by soldering for example (block 400). If the packaged IC device is coupled to a socket, a logical binding should exist between the socket and the packaged IC device. During initialization, the boot block memory unit loads and records its boot block identifier into memory of the TPM (block 410). Next, the boot block memory unit locates and loads the BIOS for execution (block 420). The BIOS (or a representation thereof) is provided to the TPM and a BIOS identifier is recorded (blocks 430 and 440). Thereafter, the BIOS loads its extensions and the OS Loader and provides these extensions and OS Loader (or representations thereof) to the TPM for recordation,

respectively (blocks 450, 460, 470 and 480). Thereafter, the BIOS passes control to the OS Loader (block 490).

Thereafter, the TPM can response to inquiry requests from a challenger to determine that the platform has been initialized and is trusted. The term "trusted" means that the platform should behave in an expected manner for an intended purpose.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to which the invention pertains are deemed to lie within the spirit and scope of the invention.

CLAIMS

What is claimed is:

1. An integrated circuit device comprising:

a package;

a trusted platform module covered by the package; and

a boot block memory unit in communication with the trusted platform module and covered by the package, the boot block memory unit to provide boot information to the trusted platform module.

2. The integrated circuit device of claim 1, wherein the trusted platform module and the boot block memory unit are employed on a single integrated circuit.

3. The integrated circuit device of claim 1, wherein the boot information includes an image of a boot block code.

4. The integrated circuit device of claim 1, wherein the trusted platform module includes a processor and a memory.

5. The integrated circuit device of claim 4, wherein the trusted platform module performs a hash operation on the boot information to produce a boot block identifier for storage within the memory.

6. The integrated circuit device of claim 5, wherein the boot block memory unit locates a basic input/output system (BIOS) and loads the BIOS into the trusted platform module.

7. The integrated circuit device of claim 6, wherein the trusted platform module performs a hash operation on the BIOS to produce a BIOS identifier for storage within the memory.

8. The integrated circuit device of claim 4, wherein the trusted platform module performs a hash operation on a basic input/output system (BIOS) extension to produce an extension identifier for storage within the memory.

9. The integrated circuit device of claim 4, wherein the trusted platform module performs a hash operation on an Operating System (OS) loader to produce an OS identifier for storage within the memory.

10. A platform comprising:

a processor;

an input/output control hub coupled to the processor; and

an integrated circuit device coupled to the input/output control hub, the integrated circuit device including

a package,

a trusted platform module covered by the package, and

a boot block memory unit in communication with the trusted platform module and covered by the package, the boot block memory unit to provide boot information to the trusted platform module.

11. The platform of claim 10, wherein the trusted platform module and the boot block memory unit of the integrated circuit device are employed on a single integrated circuit.

12. The platform of claim 10, wherein the boot information provided by the boot block memory unit of the integrated circuit device includes an image of a boot block code.

13. The platform of claim 10, wherein the trusted platform module of the integrated circuit device includes an internal memory.

14. The platform of claim 13, wherein the trusted platform module of the integrated circuit device performs a hash operation on the boot information to produce a boot block identifier for storage within the internal memory.

15. The platform of claim 14, wherein the boot block memory unit of the integrated circuit device locates a basic input/output system (BIOS) and loads the BIOS into the trusted platform module of the integrated circuit device.

16. The platform of claim 15, wherein the trusted platform module of the integrated circuit device performs a hash operation on the BIOS to produce a BIOS identifier for storage within the internal memory.

17. The platform of claim 13, wherein the trusted platform module of the integrated circuit device performs a hash operation on a basic input/output system (BIOS) extension to produce an extension identifier for storage within the internal memory.

18. The platform of claim 13, wherein the trusted platform module of the integrated circuit device performs a hash operation on an Operating System (OS) loader to produce an OS identifier for storage within the internal memory.

19. A method comprising:

extracting boot information by a trusted platform module from a unit located within a same integrated circuit package as the trusted platform module;

producing an identifier based on the boot information by the trusted platform module; and

recording the identifier within memory of the trusted platform module.

20. The method of claim 19 further comprising:

receiving an inquiry request; and

providing the boot information in response to the inquiry request.

21. The method of claim 19 further comprising:
locating a basic input/output system (BIOS);
providing the BIOS to the trusted platform module;
performing a hash operation on the BIOS to produce a BIOS identifier; and
storing the BIOS identifier in memory of the trusted platform module.

22. The method of claim 21 further comprising:
locating an operating system (OS) loader;
providing the OS loader to the trusted platform module;
performing a hash operation on the OS loader to produce a loader identifier; and
storing the loader identifier in memory of the trusted platform module.

23. A software module loaded in internal memory for execution by a trusted platform module of a platform, the software module comprising:

code to extract boot information from a memory located within a same integrated circuit package as the trusted platform module; and

code to produce an identifier based on the boot information and record the identifier within the internal memory of the trusted platform module.

24. The software module of claim 23 further comprising:
code to detect an inquiry request; and
code to output the boot information from the integrated circuit package in response to the inquiry request.

25. The software module of claim 23 further comprising:

code to locate a basic input/output system (BIOS) and to provide the BIOS to the trusted platform module;

code to perform a hash operation on the BIOS to produce a BIOS identifier; and

code to store the BIOS identifier within the internal memory of the trusted platform module.

26. The software module of claim 23 further comprising:
code to locate an operating system (OS) loader;
code to provide the OS loader to the trusted platform module;
code to perform a hash operation on the OS loader to produce a loader identifier; and
code to store the loader identifier within the internal memory of the trusted platform module.

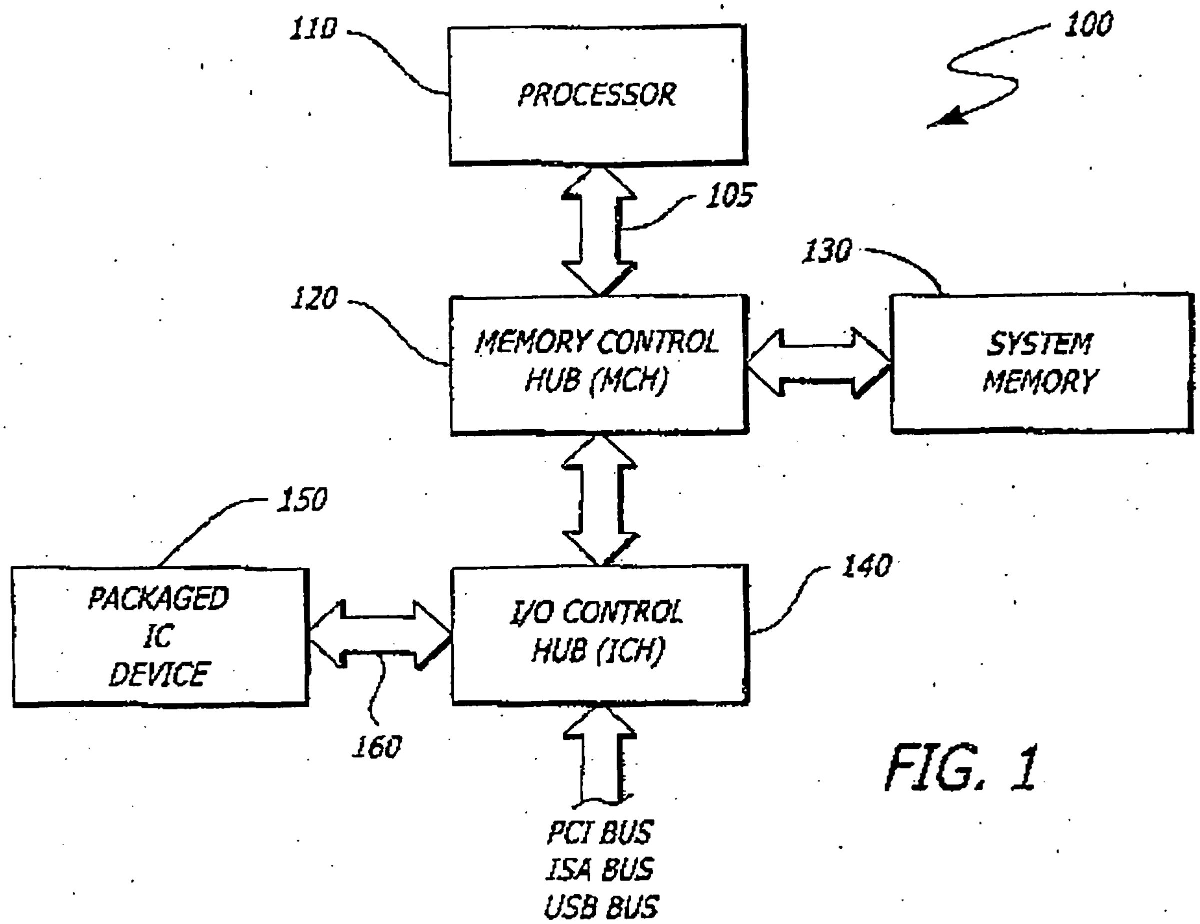

100
110
PROCESSOR
105
130
120
MEMORY CONTROL HUB (MCH)
SYSTEM MEMORY
150
PACKAGED IC DEVICE
140
I/O CONTROL HUB (ICH)
160
PCI BUS
ISA BUS
USB BUS

FIG. 1

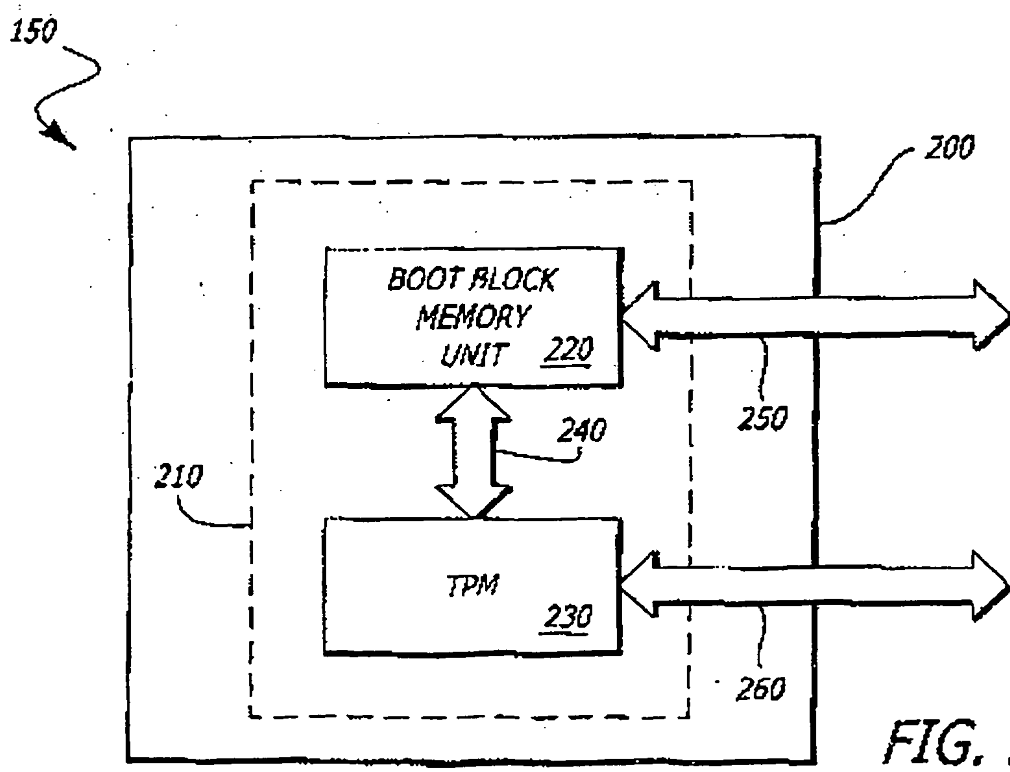

150
200
BOOT BLOCK MEMORY UNIT 220
250
240
210
TPM 230
260

FIG. 2

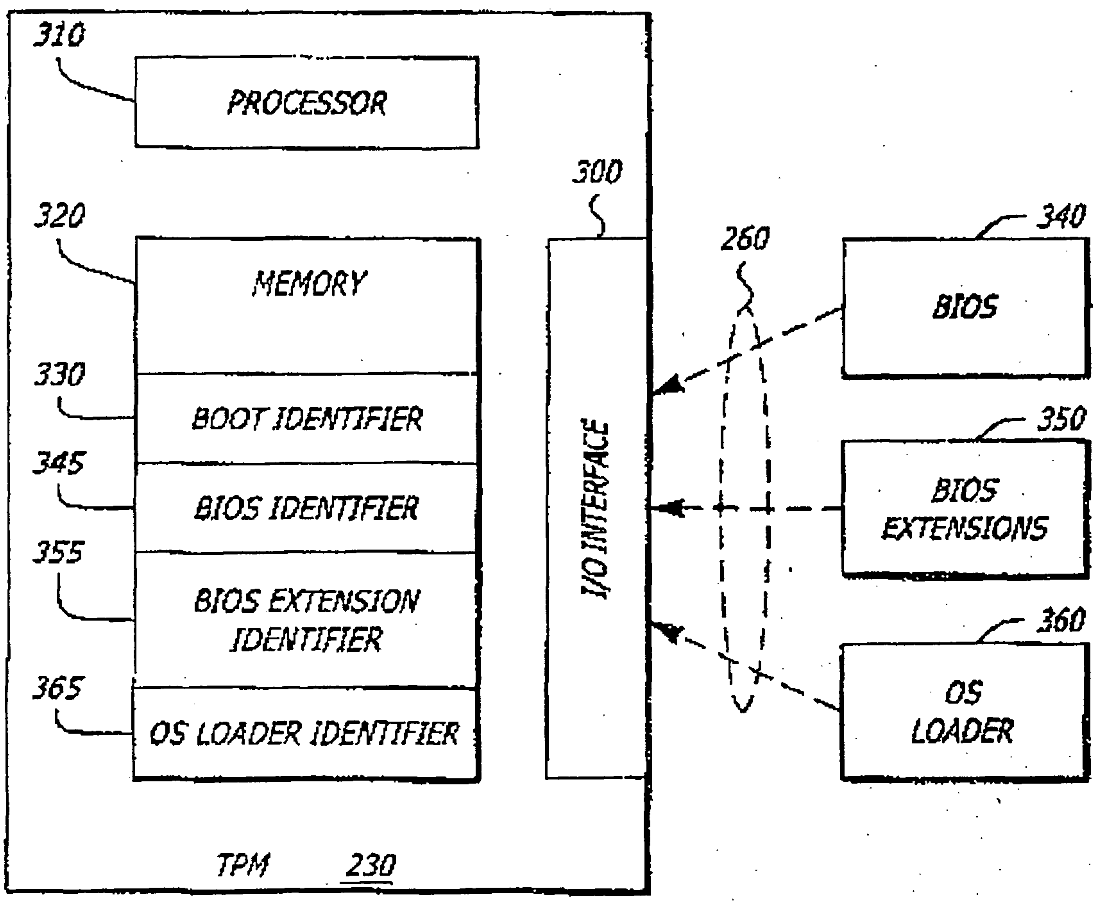

310
PROCESSOR
300
320
MEMORY
330
BOOT IDENTIFIER
345
BIOS IDENTIFIER
355
BIOS EXTENSION IDENTIFIER
365
OS LOADER IDENTIFIER
I/O INTERFACE
TPM 230
260
340
BIOS
350
BIOS EXTENSIONS
360
OS LOADER

FIG. 3

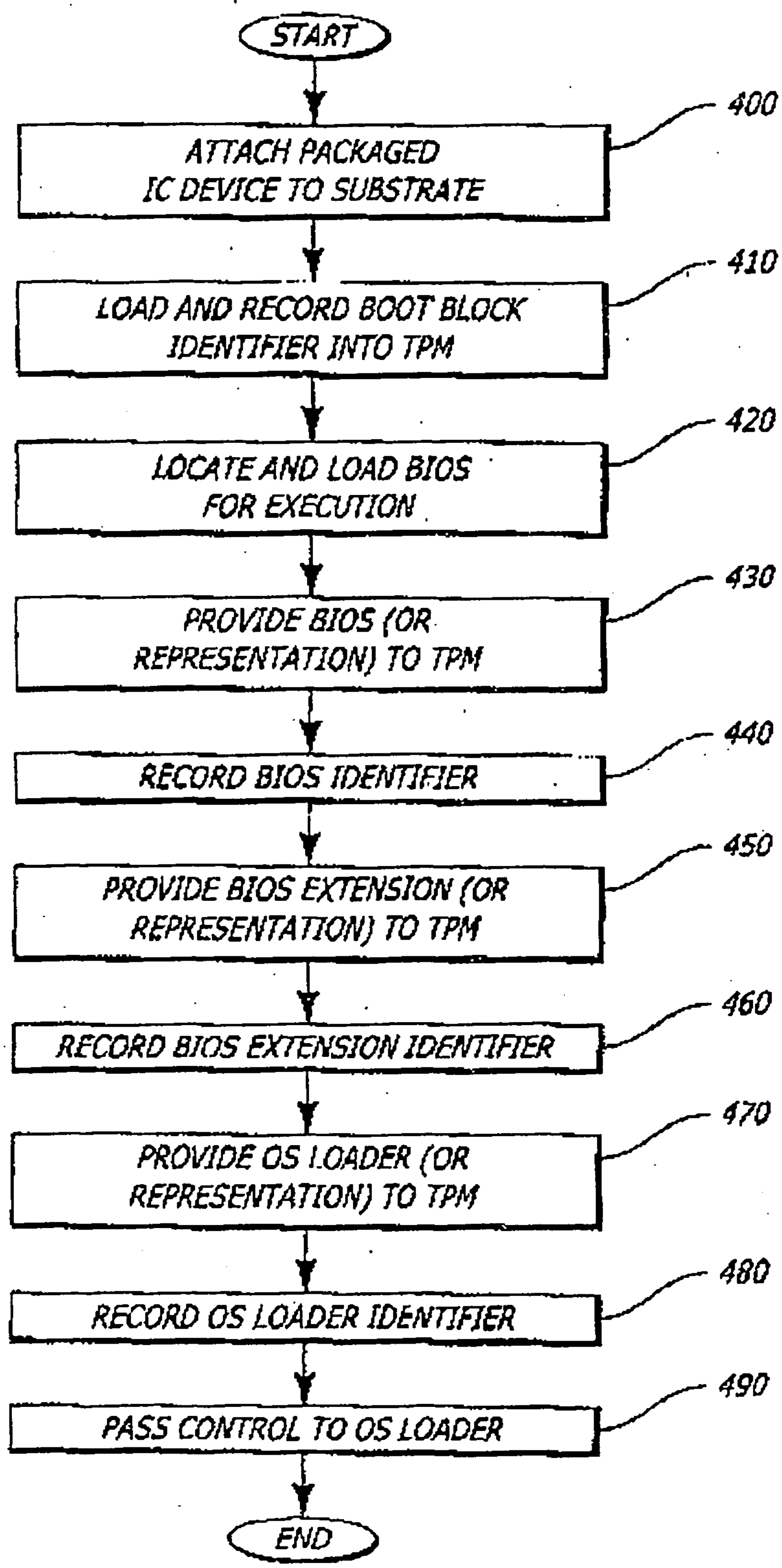

START
ATTACH PACKAGED IC DEVICE TO SUBSTRATE
400
LOAD AND RECORD BOOT BLOCK IDENTIFIER INTO TPM
410
LOCATE AND LOAD BIOS FOR EXECUTION
420
PROVIDE BIOS (OR REPRESENTATION) TO TPM
430
RECORD BIOS IDENTIFIER
440
PROVIDE BIOS EXTENSION (OR REPRESENTATION) TO TPM
450
RECORD BIOS EXTENSION IDENTIFIER
460
PROVIDE OS LOADER (OR REPRESENTATION) TO TPM
470
RECORD OS LOADER IDENTIFIER
480
PASS CONTROL TO OS LOADER
490
END

FIG. 4

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2002 (10.01.2002)

PCT

(10) International Publication Number
WO 02/003196 A3

(51) International Patent Classification[7]: G06F 9/445, 1/00

(21) International Application Number: PCT/US01/19325

(22) International Filing Date: 14 June 2001 (14.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/608,551 30 June 2000 (30.06.2000) US

(71) Applicant *(for all designated States except US)*: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: GRAWROCK, David [US/US]; 8285 Southwest 184th Avenue, Aloha, OR 97007 (US).

(74) Agent: MALLIE, Michael, J.; Blakely, Sokoloff, Taylor & Zafman, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

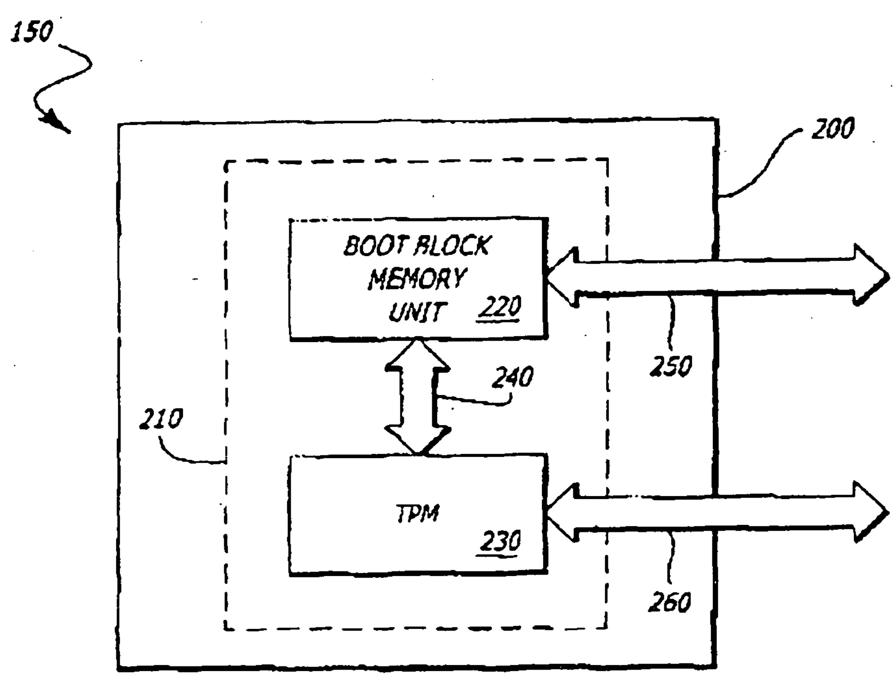
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report: 20 March 2003

[Continued on next page]

(54) Title: PROTECTION OF BOOT BLOCK DATA AND ACCURATE REPORTING OF BOOT BLOCK CONTENTS



(57) Abstract: In one embodiment, an integrated circuit device comprises a trusted platform module and a boot block memory unit covered by a common package. The boot block memory unit is in communication with the trusted platform module and provides boot information to the trusted platform module. An example of the boot information includes a boot block code.

WO 02/003196 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

I al Application No
PCT/US 01/19325

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F9/445 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 421 006 A (HANLEY NORA E ET AL) 30 May 1995 (1995-05-30) column 7, line 51 -column 9, line 54 ---	1-26
A	WO 00 10283 A (HANNAH ERIC C ;INTEL CORP (US)) 24 February 2000 (2000-02-24) page 3, line 25 -page 5, line 30 ---	1-26
A	DE 43 15 732 C (SIEMENS NIXDORF INF SYST) 1 June 1994 (1994-06-01) column 2, line 23 -column 3, line 19 -----	1-26

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 November 2002	10/12/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bijn, K

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 01/19325

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5421006	A	30-05-1995	NONE		
WO 0010283	A	24-02-2000	AU	5479799 A	06-03-2000
			WO	0010283 A1	24-02-2000
DE 4315732	C	01-06-1994	DE	4315732 C1	01-06-1994